国 际 电 信 联 盟

ITU-T X.1216

(09/2020)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

网络空间安全 – 网络安全

收集和保存网络安全事件证据的要求

ITU-T X.1216建议书

国际电信联盟

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	**X.1200–X.1229**
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1360–X.1369
智能交通系统（ITS）安全	X.1370–X.1389
分布式账簿技术安全	X.1400–X.1429
分布式账簿技术安全	X.1430–X.1449
安全协议（2）	X.1450–X.1459
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
5G 安全	X.1800–X.1819

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1216建议书

收集和保存网络安全事件证据的要求

摘要

ITU-T X.1216建议书阐述了网络安全事件响应和调查的一般程序，分析了网络安全事件证据的来源，并规定了调查过程中用于收集和保存此类证据的工具的能力要求。本建议书还规定了这些工具的可靠性保证要求，作为工具设计开发人员导则。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1216	2020-09-03	17	11.1002/1000/14259

关键词

网络安全、网络安全事件证据、事件响应和调查。

* 欲查阅建议书，请在您的网络浏览器地址域键入 URL http://handle.itu.int/，随后输入建议书的唯一ID，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联已收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1216 建议书

收集和保存网络安全事件证据的要求

1 范围

本建议书阐述了网络安全事件响应和调查的一般程序，分析了网络安全事件证据的来源，并规定了调查过程中用于收集和保存此类证据的工具的能力要求。本建议书还规定了这些工具的可靠性保证要求，作为工具设计开发人员导则。

本建议书不包含与收集网络安全事件数据、法律诉讼、纪律程序以及与处理潜在网络安全事件证据的其他行动相关的隐私问题和法规。我们认为这些内容不属于“收集和保存”的范围。

2 参考文献

下列ITU-T建议书及含有本建议书引用条款的其它参考文献构成本建议书的条款。所注明版本在出版时有效。所有建议书及其它参考文献均可能进行修订；因此鼓励建议书的使用方了解使用最新版本的下列建议书和其它参考文献的可能性。ITUT-T建议书的现行有效版本清单定期出版。本建议书在引用某一独立文件时，并未给予该文件建议书的地位。

无。

3 定义

3.1 他处定义的术语

本建议书使用了下列他处定义的术语：

3.1.1 收集（collection）[b-ISO/IEC 27037]：收集包含潜在数字证据的实物项的过程。

3.1.2 证据（evidence）[b-ITU-T X.813]：证据信息，其自身或当与其他信息一起使用时，可用于解决争议。

3.1.3 调查（investigation）[b-ISO/IEC 27042]：应用检查、分析和解释等帮助理解事故。

3.1.4 保存（preservation）[b-ITU-R BR.1351]：必须执行的维护操作，目的是确保归档材料得到适当保存，例如定期检查媒质的损坏状态并在有需要时重新在新媒质上生成内容。

3.1.5 安全事件（security incident）[b-ITU-T E.409]、[b-IETF RFC 2828]：使安全的某个方面受到威胁的任何有害事件。

3.1.6 时间戳（timestamp）[b-ISO/IEC 27037]：代表与共同时间参考相关的时间点的时间变量参数。

3.2 本建议书定义的术语

本建议书定义了下列术语：

3.2.1 网络安全事件证据（cybersecurity incident evidence）：以二进制形式存储或传输的信息或数据，通过分析过程确定其与网络安全事件调查相关。

注 – 此定义基于ISO/IEC 27037中关于“数字证据”的定义。

3.2.2 移动目标防御（moving target defence）：为使对手无法预测系统的攻击面，自动改变一个或多个系统属性的机制。

注 – 此定义基于[b-Jajodia14]。

4 缩写词和首字母缩略语

本建议书使用了下列缩写词和首字母缩略语：

ARP 地址解析协议

BYOD 自带设备

DLL 动态链接库

IP 网际协议

MAC 媒质访问控制

MTD 移动目标防御

PE File 可移植的可执行文件

PII 个人可识别信息

WORM 一写多读

5 惯例

在本建议书中：

关键词“要求”（is required to）指的是一项必须严格遵守的要求，如果宣称遵循本建议书，则不得违反。

关键词“应该”（should）指的是一项建议性的、并非绝对要求的要求，因此，宣称遵循本建议书时无需提及该项要求。

6 网络安全事件证据概述

6.1 事故响应和调查的一般程序

在分析网络安全事件的原因时，收集和保存与该事件相关的证据是应对和调查事件的重要组成部分，因为所分析的网络安全事件数据可能成为法庭审判案件的潜在证据。此外，收集的网络安全事件证据可用于检查漏洞，以增强相关组织的网络安全。

图1所示的事故调查程序包括以下连续阶段：

- 准备：在此阶段，应对事件调查进行初步准备。
- 检测：在此阶段，会观察到未经授权的情况，即事件。根据事件的严重程度，除收集数据外，还应决定如何应对此事件。

- 收集：数据应从用于收集流量数据的工具中获取。这个阶段非常重要，因为流量数据交换速度很快，以后不可能生成相同的网络流量数据。
- 保存：获得的原始网络流量数据应存储在备份设备上，所有数据的散列亦应保存。
- 调查：在此阶段，收集的所有痕迹都应整合。对证据进行搜索，以识别攻击手段。使用现有攻击模式对指标进行分类和关联，从而推断出重要的观察结果。此方法可以确定攻击的路径，且属性可通过在该阶段执行迭代分析确定攻击者的身份，以得出结论。
- 报告：调查的观察结果和解释应以法律人士可以理解的语言呈现。

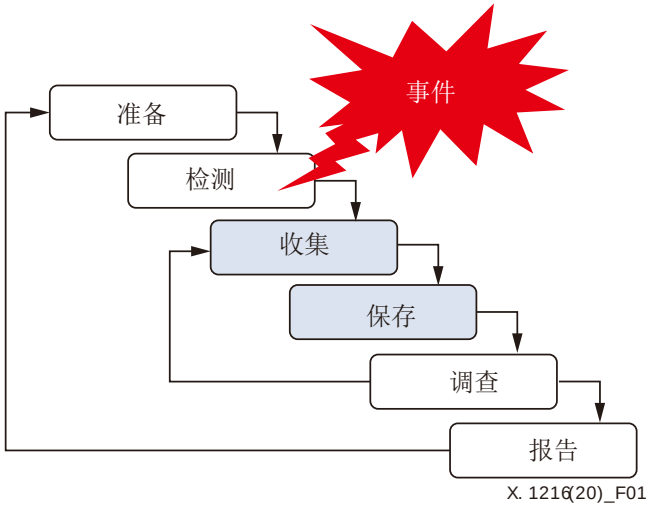

图1 – 事件调查的一般程序

与数字调查和事件响应相关的各种ISO/IEC导则在[b-ISO/IEC 27035-3、b-ISO/IEC 27037、b-ISO/IEC 27041、b-ISO/IEC 27042、b-ISO/IEC 27043]中实现了标准化。这些导则主要致力于在整个事件调查过程中提供最佳实践和处理数字证据。[b-IETF RFC 3227]亦介绍了证据收集和归档导则，例如收集步骤的准备和考虑；为监管链选择归档使用的媒介和文件；证据收集和归档所需的工具集。然而，我们并未明确提供有关选择或开发调查工具的导则。

6.2 网络安全事件的数据源

与网络安全事件相关的典型数据源包括主机设备、网络安全设备、网络设备和网络。图2描述了数据源提供的可用分类信息。

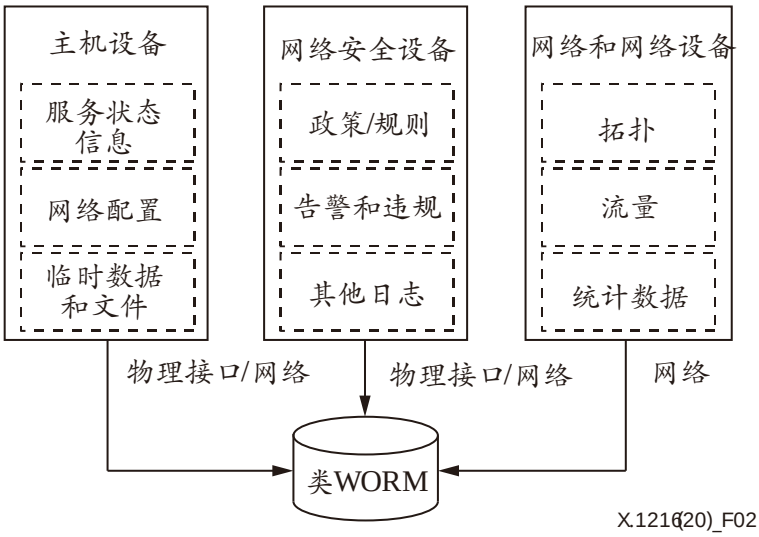

图2 – 获取网络安全事件数据的各种来源

6.2.1 主机设备

通常，主机设备提供与网络安全事件相关的各种数据。数据收集工具应该仔细收集这些数据，因为其中一些数据并不稳定，很容易销毁。可从主机设备收集的数据类型如下：

(1) 与系统状态相关的数据：

- 一般信息（主机名、用户账户信息、系统日期和时间、上次启动时间、当前时区、启动设备）；
- 操作系统信息（制造商、名称、体系架构、版本、序列号、安装日期）；
- 应用程序（已安装的程序、补丁的状态、环境变量）；
- 流程（流程表、自动运行的流程、预定的服务）；
- 登录会话；
- 其他注册表数据。

(2) 数据和与存储相关的数据：

- 内存数据；
- 临时文件系统（最近使用或执行的文件，包括动态链接库（DLL）和句柄）；
- 隐藏文件、可执行文件、打开的文件、删除的文件、未分配的区域；
- 档案媒质；
- 共享数据（共享文件夹、网络设备）。

(3) 与网络相关的数据：

- 路由表、ARP缓存、内核统计；
- 网络配置（IP地址、MAC地址、开放端口、网络接口）；
- 与互联网浏览器相关的信息（互联网浏览器的历史信息、最近访问的互联网对象、cookies）。

6.2.2 网络安全设备

应该从网络安全设备（如入侵检测系统和防火墙）收集与攻击活动相关的数据。

- 安全策略（访问控制、检测规则）；
- 安全事件和日志（警报、告警、警告、错误）；
- 统计信息。

6.2.3 网络和网络设备

调查网络攻击时，从网络收集数据非常重要。特别是网络拓扑信息可以帮助网络事件调查员了解企业网络的组件和配置，发现攻击路径并估计损坏的程度。在网络配置随着云计算、虚拟机、自带设备（BYOD）和基于移动目标防御（MTD）安全技术的部署而动态变化时，尤为明显。网络和网络设备数据的典型实例包括：

- 网络拓扑配置；
- 路由器日志；
- 网络化服务；
- 与网络化主机相关的信息（开放端口、内部运行服务、状态）；
- 流量跟踪，包括报头和数据；
- 会话流数据（源IP地址/端口号、目的地IP地址/端口号、协议、其他TCP报头信息）；
- 通过网络传输的文件；
- 网络流量统计。

7 收集网络安全事件数据的要求

与决定需要收集什么数据同样重要的是在发生网络安全事件时，决定如何收集、保存和分析这些数据。本节描述了从第6节介绍的三类数据源收集网络安全事件数据的能力。

从数据源收集的日志和其他事件数据可能包括个人身份信息（PII）。收集者应尽量减少收集任何PII，仅收集绝对必要的事件报告和事件响应信息，并根据相关的适用法律法规保护PII。

7.1 从主机设备收集网络安全事件数据

主机设备通常是网络安全事件分析的主要数据源。这些设备提供与系统加载的注册表、日志和文件相关的数据。当需要更精确分析时，应从主机设备收集内存转储数据。

为支持此操作，收集工具应该具有下列功能：

– 检查过程并收集过程信息；
– 收集系统状态；
– 进行逐位复制；
– 生成核心图像；
– 实现收集过程自动化；
– 导入和导出收集的数据；

– 支持主机设备的各种操作系统；
– 提供收集数据所需的库且不使用主机设备的任何库；
– 在系统运行时收集易变数据；以及
– 收集当前连接和已打开插座的网络状态。

7.2 从网络安全设备收集网络安全事件数据

应从入侵保护系统、入侵检测系统、入侵防御系统、防火墙系统、安全信息和事件管理系统等网络安全设备，获得大量对网络安全事件分析有用的数据。

为支持此操作，收集工具应该具有下列功能：

– 从网络安全设备收集事件日志；
– 从网络安全设备收集警报和违规日志；
– 从网络安全设备收集用户身份认证日志；以及
– 收集网络安全设备的安全策略和规则。

7.3 从网络和网络设备收集网络安全事件数据

相关组织收集证据并进行网络监控，以识别内部同谋的疑点。如果基于主机的监控无效，网络监控可以提高证据的有效性。网络监控不是为了防止攻击，而是为在事件发生时收集相关信息，并为分析提供更多证据。要从网络和网络设备收集安全事件数据，数据收集工具应提供以下功能：

- 无损耗地收集网络流量；
- 从网络跟踪中提取会话流并收集会话流信息，如源IP地址和端口号、目标IP地址和端口号、IP协议和服务信息、会话的开始和结束时间、入局数据包的数量和大小、出局数据包的数量和大小；
- 收集通过网络传输的可移植的可执行文件并提取文件信息，如文件名、文件大小、文件的收集时间、包含可移植文件会话的源IP地址和端口号、包含可移植文件会话的目标IP地址和端口号、IP协议；
- 收集路由器、交换机、网络监控系统等网络设备的日志。

8 网络安全事件的数据保存要求

为分析网络安全事件的原因，有必要保存收集到的原始数据并避免其潜在的损害。特别是在考虑法律案件时，有必要保存收集的数据，以保持证据的完整性和合法性。为支持上述要求，保存工具应具备以下功能：

– 生成校验和及数字签名；
– 验证收集的数据保存完好无损；
– 生成数据收集和保存时间的时间戳（单位：毫秒）；
– 将收集的数据记录于一写多读（WORM）设备；
– 提供应加以相应维护的数据保留策略特征；
– 确保收集的数据在策略持续期间得以保存；以及
– 以正式的形式保存收集的数据和元数据。

9 为确保可靠性提出的收集和保存工具要求

利用收集保存工具收集并保存的数据可用于调查网络安全事件的原因，并作为确定事件责任的证据。

因此，收集和保存网络安全事件分析数据的工具，应提供包括用户管理和数据管理在内的以下可靠性保证功能：

- 该工具应提供一种手段，用于限制和控制用户对工具本身和存储数据的访问；
- 在未经适当授权的情况下，该工具不得允许尝试覆盖、更改或删除保留数据；
- 该工具应提供安全管理功能，规定授权管理员可以配置并管理安全功能、安全策略和重要数据；
- 在处于物理分离状态的设备之间传输所收集数据时，必须对数据进行加密，以确保机密性和完整性；
- 与工具相关的所有通信手段应使用安全加密通信协议；
- 该工具应为保存的数据提供备份功能；
- 该工具应提供日志记录、错误报告和审计功能；以及
- 该工具应提供处理元数据和正式内容并根据现有策略进行共享的功能（如[b-ITU-T X.1550]和[b-ITU-T X.1582]中的规定）。

参考书目

[b-ITU-T E.409] ITU-T E.409 (2004)建议书，事件组织和安全事件处理：电信组织导则。

[b-ITU-T X.813] ITU-T X.813 (1996)建议书，信息技术－开放系统互连－开放系统的安全框架：不可否认框架。

[b-ITU-T X.1215] ITU-T X.1215 (2019)建议书，结构化威胁信息交换的用例。

[b-ITU-T X.1541] ITU-T X.1541 (2017)建议书，事件对象描述交换格式2。

[b-ITU-T X.1550] ITU-T X.1550 (2017)建议书，事件交换网络的访问控制模型。

[b-ITU-T X.1582] ITU-T X.1582 (2014)建议书，支持网络安全信息交换的传输协议。

[b-ITU-R BR.1351] ITU-R BR.1351 (1998)建议书，将数字技术应用于无线电广播的音频归档系统的要求。

[b-IETF RFC 2828] IETF RFC 2828 (2000), *Internet Security Glossary*.

[b-IETF RFC 3227] IETF RFC 3227 (2002), *Guidelines for Evidence Collection and Archiving.*

[b-ISO/IEC 27035-3] ISO/IEC 27035-3, *Information technology −Security techniques − Information security incident management −Part 3: Guidelines for incident response operations.*

[b-ISO/IEC 27037] ISO/IEC 27037:2012, *Information technology −Security techniques − Guidelines for identification, collection, acquisition and preservation of digital evidence.*

[b-ISO/IEC 27041] ISO/IEC 27041:2015, *Information technology −Security techniques − Guidance on assuring suitability and adequacy of incident investigative method.*

[b-ISO/IEC 27042] ISO/IEC 27042:2015 *Information technology −Security techniques − Guidelines for the analysis and interpretation of digital evidence.*

[b-ISO/IEC 27043] ISO/IEC 27043: 2015, *Information technology −Security techniques − Incident investigation principles and processes.*

[b-Jajodia14] Jajodia, Sushil, and Kun Sun. "MTD 2014: First ACM workshop on moving target defense." Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. 2014.

ITU-T 系列建议书

系列 A	ITU-T 工作的组织
系列 D	资费及结算原则和国际电信/ICT 的经济和政策问题
系列 E	综合网络运行、电话业务、业务运行和人为因素
系列 F	非话电信业务
系列 G	传输系统和媒介、数字系统和网络
系列 H	视听及多媒体系统
系列 I	综合业务数字网
系列 J	有线网络和电视、声音节目及其他多媒体信号的传输
系列 K	干扰的防护
系列 L	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列 M	电信管理，包括 TMN 和网络维护
系列 N	维护：国际声音节目和电视传输电路
系列 O	测量设备的技术规范
系列 P	电话传输质量、电话设施及本地线路网络
系列 Q	交换和信令，以及相关的测量和测试
系列 R	电报传输
系列 S	电报业务终端设备
系列 T	远程信息处理业务的终端设备
系列 U	电报交换
系列 V	电话网上的数据通信
系列 X	**数据网、开放系统通信和安全性**
系列 Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列 Z	用于电信系统的语言和一般软件问题

瑞士印刷
2020年，日内瓦